CLAIMS

What is claimed is:

1. An apparatus comprising:

a network interface module to connect the apparatus to a network;

a packet capture module to intercept packets being transmitted on the network;

an object assembly module to reconstruct objects being transmitted on the network from the intercepted packets;

an object classification module to determine a type of content of the reconstructed objects;

an object store module to store the objects; and

a user interface to enable a user to search objects stored in the object store module.

2. The apparatus of claim 1, wherein the object assembly module comprises a reassembler to assemble the intercepted packets into flows.

3. The apparatus of claim 2, wherein the object assembly module further comprises a protocol demultiplexer to sort the assembled flows by protocol.

4. The apparatus of claim 3, wherein the object assembly module further comprises a protocol classifier to extract the objects from the sorted assembled flows.

5. The apparatus of claim 1, wherein the object classification module determines whether objects are stored in the object store or discarded based on one or more capture rules.

6. The apparatus of claim 5, wherein the capture rules are user-configurable through the user interface.

7. The apparatus of claim 1, wherein the object classification module determines a location that each object is stored in the object store based on the type of content of each object.

8. The apparatus of claim 1, wherein the object classification module determines the type of content of each object using a signature of each object.

9. The apparatus of claim 1, wherein the user interface comprises a graphical user interface.

10. The apparatus of claim 1, wherein the object store module comprises a content store to store the objects and a tag store to index the objects stored in the object store.

11. The apparatus of claim 10, wherein the content store comprises a canonical storage, and the tag store comprises a database.

12. An method comprising:

intercepting data being transmitted on a network;

reconstructing objects being transmitted on the network from the intercepted data;

classifying the reconstructed objects by content type;

storing the classified objects; and

indexing the stored objects to enable searching of the stored objects.

13. The method of claim 12, wherein reconstructing the objects comprises:

sorting the intercepted data into packets;

assembling the packets into flows; and

sorting the assembled flows by protocol.

14. The method of claim 12, further comprising determining whether each object is to be stored based on a set of one or more capture rules.

15. The method of claim 12, further comprising receiving a query over the stored objects.

16. The method of claim 15, further comprising searching the indexed objects, and retrieving objects matching the query.

17. An machine-readable medium having stored thereon data representing instructions that, when executed by a processor, cause the processor to perform operations comprising:

intercepting data being transmitted on a network;

reconstructing objects being transmitted on the network from the intercepted data;

classifying the reconstructed objects by content type;

storing the classified objects; and

indexing the stored objects to enable searching of the stored objects.

18. The machine-readable medium of claim 17, wherein reconstructing the objects comprises:

sorting the intercepted data into packets;

assembling the packets into flows; and

sorting the assembled flows by protocol.

19. The machine-readable medium of claim 17, wherein the instructions further cause the processor to determine whether each object is to be stored based on a set of one or more capture rules.

20. The machine-readable medium of claim 17, wherein the instructions further cause the processor to receive a query over the stored objects, search the indexed objects in response to the query, and retrieve objects matching the query.